

# **ABSTRACT**

An objective is to obtain a Jacobian group element adder that can calculate addition in a Jacobian group of a  $C_{ab}$  curve at a high speed, and can enhance practicality of the  $C_{ab}$  curve.

An algebraic curve parameter file A 10, and Groebner bases  $I_1$  and  $I_2$  of ideals of a coordinate ring of an algebraic curve designated by this file A are input into an ideal composition section 11 to perform arithmetic of producing a Groebner basis J of an ideal product of the ideal generated by  $I_1$  and ideal generated by  $I_2$ . In a first ideal reduction section 12, arithmetic is performed of producing a Groebner basis  $J^*$  of an ideal that is smallest in a monomial order designated by the file A among ideals equivalent to an inverse ideal of an ideal that J in the coordinate ring of the algebraic curve designated by the file A generates. In a second ideal reduction section 13, arithmetic is performed of producing a Groebner basis  $J^{**}$  of a ideal that is smallest in the monomial order designated by the file A among ideals equivalent to an inverse ideal of an ideal that this  $J^*$  generates to output it.